[19]中华人民共和国专利局

[51]Int.Cl[6]
H04B 10/02

[12] 发明专利申请公开说明书

[21] 申请号 96121571.2

[43]公开日 1997 年 9 月 10 日

[11] 公开号 CN 1159108A

[22]申请日 96.12.18

[30]优先权

[32]95.12.18[33]FR[31]9514988

[71]申请人 阿尔卡塔尔CIT有限公司

地址 法国巴黎

[72]发明人 胡伯特·米奥内特 皮埃尔·海尔梅特 马克·迪乌东尼

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

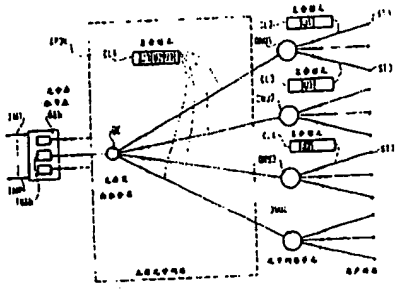
代理人 陆立英

权利要求书 3 页 说明书 18 页 附图页数 5 页

[54]发明名称 用在异步传输模式信元传送信息的加密和解密器件

[57]摘要

一种加密器件可以用来对由一个无源光学网络从一个光学传播节点到各网络单元的信元传递的信息单元加密。每个信元至少传递一个信息单元而每个信息单元被分别送往一个用户终端。该装置包括一个加密系统，能用明文从至少一个位于网络单元的解密器件处至少接收一个密钥应用。包括 ATM 电信网络。



权 利 要 求 书

1. 对异步传输方式信元传送的信息单元加密的加密器件（CD）使用在一种光学分布网络中. 该种网络包括一个光学存取节点（OAN）、一个定向无源光学网络（APON）和许多网络单元（ONU1、…、ONU4）. 耦合装置（DC）只将一个网络单元（ONU1、…、ONU4）发送的任何信元传送到光学存取节点（OAN），信元从一个节点（OAN）向网络单元（ONU1、…、ONU4）传播，每个信元至少传递一个信息单元（U1、U2、U3），每个信息单元被送往一个单独的网络单元（ONU1、…、ONU4）；

上述加密器件（CD）位于所说的光学存取节点（OAN）中并包括:

-根据一个第一伪随机序列（NLS1）的一个相应位为每个要加密的信息单元的每一位计算一个加密值的装置（EXOR1）；以及

-按照信息单元被送往的网络单元所特有的一个密钥值（Ki）供应该第一伪随机序列的装置（NLF1、SD1、CDC）；

特征在于: 供应该第一伪随机序列（NLS1）的装置（NLF1、SD1、CDC）包括:

-根据一个密钥值（Ki）使用一种很难逆运算的算法对该此第一伪随机序列（NLS1）进行计算的装置（NLF1）；以及

-从网络单元的至少一个解密器件（DD）以明文接收至少一个键（Ki）的装置（KM、CDC）.

2. 根据权利要求1的加密器件，对于每个传递许多分别送往许多分立的、但都连到同一个网络单元（ONU1）的用户终端（ST1、ST3）的信息单元（U1、U3）的复合信元来说，其特征在于第一伪随机序列（NLS1）也由本信息单元在加密后运送它的信元中的位置（BP）所决定.

3. 根据权利要求1的加密器件，其特征在于第一伪随机序列也是根据构成同步序列的第二伪随机序列（LS1i）计算的，同时也在于供给第一伪随机序列（NLS1）的装置还包括供给第二伪随机二进制序列（LS

1 i）和发送该序列的取样到至少一个解密器件（DD）以使其同步的同步装置.

4. 根据权利要求3的加密器件，其特征在于供给一个第二伪随机序列（SD1 i）的装置（SD1）供给一个与在节点和一个网络单元之间建立的每个虚拟电路无关的第二序列，也在于供给此序列的定时率相应于信元在有关虚拟电路上发送的速度.

5. 根据权利要求3的加密器件，其特征在于供给一个第二伪随机序列（LS1 i）的装置（SD1）包括一个移位寄存器（Q1、…、Q25），后者和一个运算一线性函数的逻辑电路构成回路，也在于提供的取样包含有在该移位寄存器的至少一级中含有的值（S1、S2）.

6. 根据权利要求1的加密器件，其特征在于它还包括有装置（KM，CDC）用于:

- 存储许多密钥、
- 决定改变密钥、和
- 在每个信元中插入信息，指出用哪个密钥对该信元中传送的信息单元进行加密.

7. 解密器件（DD）用于对异步传输方式的信元所传送的信息单元进行解密，可用在定向无源光学网络（APON）中. 后者包括一个光学存取接点（OAN）、许多网络单元（ONU1、…、ONU4）和耦合装置（DC），将每个由节点发送出来的任何信元从节点向网络单元传播，而只将一个网络单元发送的任何信元传送给节点处；每个信元至少传递一个信息单元（U1、U3），而每个信息单元只送往一个网络单元;

上述解密器件（DD）位于一个网络单元并包括:

- 根据一个第一伪随机序列（NLS2）的一个相应位计算每个要解密的信息单元的每一位的一个解密值的装置（EXOR2）；以及
- 根据包括上述的解密器件的网络单元供给此第一伪随机序列的装置（NLF2、SD2、DDC）;

其特征在于供给此第一伪随机序列（NLS2）的装置（NLF2、SD2、DDC）包括:

- 根据一个密钥值（Ki）使用一种很难逆运算的算法对此第一伪随

机序列（ＮＬＳ２）进行计算的装置（ＮＬＦ２）；以及

－供给此密钥值（Ｋｉ）并将其用明文送至一个位于光学存取节点（ＯＡＮ）处的一个加密器件的装置（ＫＲ、ＤＤＣ）.

8. 根据权利要求7的解密器件，对于每个传送分别送往许多分立的、但都连到同一个网络单元（ＯＮＵ１）的用户终端（ＳＴ１、ＳＴ３）的大量信息单元（Ｕ１、Ｕ３）的复合信元来说，其特征在于第一伪随机序列（ＮＬＳ２）和该信息单元在传送它到解密器件的信元中的位置（ＢＰ）有关.

9. 根据权利要求7的解密器件，其特征在于第一伪随机序列（ＮＬＳ２）也是根据构成一个同步序列的第二伪随机序列（ＬＳ２ｉ）计算的，同时也在于供给第一伪随机序列（ＮＬＳ２）的装置还包括供给此第二伪随机二进制序列（ＬＳ２ｉ）和使该序列在由一个加密装置（ＣＤ）提供的该序列的取样的基础上成为同步的同步装置（ＳＤ２）.

10. 根据权利要求9的解密器件，其特征在于供给一个第二伪随机序列（ＳＤ２ｉ）的装置（ＳＤ２）供给与在节点和网络单元之间建立的每个虚拟电路无关的一个第二序列，也在于供给此序列的速度相应于信元在有关虚拟电路上被接收的速度.

11. 根据权利要求9的解密器件，其特征在于供给一个第二伪随机序列（ＬＳ２ｉ）的装置（ＳＤ２）包括一个移位寄存器（Ｑ１'、…、Ｑ２５'）并由一个运算一线性函数的逻辑电路构成回路，也在于加密装置（ＣＤ）提供的取样装入该移位寄存器的至少一级中以使之同步.

12. 根据权利要求7的解密器件，其特征在于它还包括有：

－存储许多密钥的装置（ＫＲ）；

－接收在每个被加密信元中传送的信息的装置（ＤＤＣ），该信息指出用哪个密钥对该信元中传送的信息单元进行加密；以及

－在存储装置（ＫＲ）中阅读由一个信元中传递的信息指出的密钥和将其提供给装置（ＮＬＦ２）以供给第一伪随机序列（ＮＬＳ２）的装置（ＤＤＣ）.

说　　明　　书

用在异步传输模式信元传送信息的加密和解密器件

本发明涉及用在异步传输模式（asynchronous transfer mode）信元传送信息的加密和解密器件．能够在电信网络中用一点对多点方式从节点向网络单元发送,或节点向网络单元播送信元提供加密服务．本发明特别适用在含有接到至少一个无源光学网络的至少一个光学存取节点的电信网络中．

图1表示这类电信网络分支点的一个实施例的方框图．它包含:一个光学存取节点 OAN 和无源光学网络．图 1 是以接到许多网络单元 ONU1,ONU2,ONU3,ONU4 和用户终端 ST1、....、ST12 的单个无源光学网络 APON 为例的．光学存取节点 OAN 用多路复用器 IM1、....、IMP,例如 2Mbit/s 同步多路复用器,或宽带多路复用器接到电信网络的其他节点,发送异步传输模式信元．

节点 OAN 有一个含有光学线路终端功能和用光纤接到网络 APON 的一个无源方向耦合器 DC 上的耦合器件 TUAN．同样,每个单元 ONU1、....、ONU4 用光纤接到耦合器 DC 上．光纤和耦合器 DC 组成无源星形光学网络 APON．耦合器 DC 具有把节点 OAN 发出的光学信号同等地传播到所有单元 ONU1,ONU2,ONU3,ONU4 的性能．此外,由于耦合器 DC 的方向特性,任何部件发出的光学信号都只能送到被它规定的节点 OAN．

每个网络单元 ONU1、....、ONU4 接到一个或更多个用户终端．例如单元 ONU1 用光纤,宽带电气连接或一般的窄带电气连接,接到三个用户终端 ST1,ST2,ST3．在窄带电气连接的情况,网络单元有通常的异步/同步和同步/异步转换器．

为了有效地利用异步传输模式网络的资源,设想使用复合信元,每个这样的信元传送几个送往不同用户终端的信息单元,但是至少在一段路径上用同一个信元传送．

图1表示规定复合信元CL1的例子,它是从多路复用器IM1、....、IMP收到的信息由耦合器TUAN合成的. 复合信元CL1由方向耦合器DC同等地传播到每个单元ONU1、....、ONU4中. 操作和维护的消息告知单元ONU1,信元CL1含有送往用户终端ST1的信息单元U1和送往用户终端ST3的信息单元U3,终端ST1和ST3就被连到单元ONU1上. 同样,单元ONU3知道信元CL1含有送往被连到单元ONU3上用户终端ST7的信息单元U2.在这个例中,单元ONU1从信元CL1中抽取两个信息单元,然后分别把它们转发到连接单元ONU1到用户终端ST1的光纤上的CL1和连接单元ONU1到用户终端ST3的光纤上的CL3. 单元ONU3从信元CL1中抽取信息单元U2并把它转发到连接用户终端ST7的光纤上.

在另一个例中,一个单元以同步的帧的形式把信息单元转发到将用户终端连到单元的一对铜线上.

每个信息单元可以是通常同步电话线路的上八位位组,由它在信元中的位置识别哪些是常量,或由数据微包(micropacket)中开头的标签识别出数据微包.

这类电信网络分支点有某些优点,特别是可以很容易把传播信息单元发送给所有的用户,例如播送音像节目. 但是也有缺点,每个网络单元ONU1、....、ONU4都收到从耦合器TUAN发送的所有信元,包括那些不含任何信息单元的信元也送到接在有关单元上的用户终端. 一个有网络单元的用户就会收到从耦合器TUAN发送的所有信息. 因此要设法保护那些不是送给所有用户终端的信息单元的机密.

有许多加密的方法:

- 块加密法是把指定长度的一段数据块执行加密算法,这就必需等待整个数据块完备才能加密. 数据块带着识别每块的标志发送. 因而容易加密和解密. 另外,这种方法带来正比于块的规模的加密和解密时延. 此外,最低发送误差可以使整块的解密被损害.

- "逐位"(On the fly)加密法是用异或门对发送的二进制数据流每位连续地和伪随机二进制序列每位相加得到加密的位流. 解密是用异或门对加密的数位流每位连续地和加密用相同的伪随机二进制序列每位相加. 用在加密和解密的伪随机二进制序列必需是同步的. 而且,一旦伪随机二进制序

列的同步因发送出错而丢失,就必需立即重建.

欧洲申请专利 0 374 028 叙述一个用在传送复合信息包加密信息单元的加密器件,信息包由一个光学存取节点播送到用户装置,每个用户装置被认为由一个网络单元和单个用户终端组成. 每个复合信息包传送许多信息单元,每个信息单元被派送给不同用户装置. 为了保密,每个信息单元都被加密. 每个用户装置接收到所有的信息单元,但是只有信息单元要派送的用户装置才能解密.

为了对每个信息单元加密,节点有一个逐位加密器件为信息单元每一数位根据指定用户装置的伪随机序列相应的位计算加密数值. 这个数据流简单地包含由该用户发送并被节点无误地接收的最后一个信息单元的数位. 发送到节点的信息单元是明文的,因为耦合器的方向特性阻止其他的用户装置接收它们. 用户装置发送的信息单元可能是种种色色,所以因各用户装置而不同. 节点收到每个错误的信息单元因此含有各用户装置特有的伪随机序列. 每个用户装置如果收到表示发送无误的认可,就把它发往节点最后的一个信息单元放入储存器. 用户的解密器件随即用这个信息单元作为对节点发送的下一个信息包中的信息单元解密的伪随机序列.

加密器件和解密器件用的伪随机序列是同步的,因为加密器件将它无误地接收的最后一个信息单元系统地用作伪随机序列,解密器件将它发送而又无误地被节点接收的最后一个信息单元, 系统地用作伪随机序列.

这样的加密器件和解密器件缺点是,只有在两个发送方的数据率相等,而且从节点和用户装置发送信息单元有一定的同步程度才能工作:

如果送往用户装置的信息单元的比特率大于该用户装置发送信息单元的比特率,加密器件有时会缺乏信息用以构成逐位加密需要的伪随机序列. 如果发往节点的信息单元没有插在两个发往用户装置的信息单元之间,加密器件就会缺乏信息用以构成对信息单元加密需要的伪随机序列.

因此这些先有技术的器件在异步传输模式网络中是不实用的,因为这类网络一个特性和一个优点是精细, 允许比特率大幅改变和异步操作.

本发明目的在提出没有上述缺点的一个加密器件和解密器件.

在第一个方式中,本发明由一个用来对异步传输模式传送的信息单元加密的加密器件,可以用在含有一个光学存取节点,一个定向无源光学网络和

许多网络单元,它们以只有从网络单元把任一信元送到光学存取节点的方式耦合,信元从一个节点播送到网络单元,每个信元传送至少一个信息单元,每个 信息单元送往单个网络单元;

上述加密器件装在上述光学存取节点内,包含:

- 对要加密的每个信息单元的每位数,根据第一个伪随机序列相应的位计算加密数值的装置;和

- 根据给信息单元要送往的网络单元指定的密钥数,提供这样的第一个伪随机序列的装置;

这里,提供这样的第一个伪随机序列的装置包含:

- 根据一个密钥数用难以逆运算的算法计算这样的第一个伪随机序列的装置;和

- 从网络单元里至少一个解密器件中以明文收到至少一个密钥的装置.

在第二个方式中,本发明由一个用来对异步传输模式传送的信息单元解密的解密器件,可以用在含有一个光学存取节点,一个定向无源光学网络和许多网络单元,它们以只有从网络单元把任一信元送到光学存取节点的方式耦合,信元从一个节点播送到网络单元,每个信元传送至少一个信息单元,每个 信息单元派送往单个网络单元;

上述加密器件装在上述光学存取节点内,包含:

- 对要解密的每个信息单元的每位数,根据第一个伪随机序列相应的位计算解密数值的装置;和

- 根据给信息单元要送往的网络单元指定的密钥数,提供这样的第一个伪随机序列的装置;这里,提供这样的第一个伪随机序列的装置包含:

-根据一个密钥数用难以逆运算的算法计算这样的第一个伪随机序列的装置;和

- 从网络单元里至少一个加密器件中以明文收到至少一个密钥的装置.

上述器件可以把同样的密钥供给光学存取节点和一个网络单元,密钥的机密性用以下特征的组合来保护:

-由解密器件产生密钥并把它供给加密器件.

- 以定向光学网络形式链接,保护了光学网络单元向光学存取节点方向

发送的机密性.

本发明另一个对象是复合信元的加密器件,这些信元传送许多信息单元分别派送往许多分离的而又接到同一个网络单元上的用户终端,其中第一个伪随机序列也是在信元加密后传送,由该信息单元在信元中的位置规定.

本发明另一个对象是复合信元的解密器件,这些信元传送许多信息单元分别派送往许多分离的而又接到同一个网络单元上的用户终端,其中第一个伪随机序列也是由该信息单元在送到解密器件的信元中的位置规定.

上述器件保证加强了机密性,因为加密关系到一个附加的变量:信息单元在传送它的信元中的位置.

在一个推荐的实施例中,可用在定向无源光学网络,第一个伪随机序列也是由包含同步序列的第二个伪随机序列计算出的,然后供给第一个伪随机序列的装置包含供给第二个伪随机二进制序列的同步设置,以及为了使它同步向至少一个解密器件发送该序列的样本.

第一个伪随机序列也是由包含同步序列的第二个伪随机序列计算出的,然后供给第一个伪随机序列的装置包含供给第二个伪随机二进制序列的同步设置,以及为了使这个序列在加密器件供给的该序列的样本基础上同步的设置.

于是,同步问题就用两个独立的伪随机序列解决了;第一个序列是很难模仿的,只有一个网络单元知道因而加密具有阻力. 第二个序列明白地播送到所有的网络单元,是用来作产生和复制第一个序列时的时间参考,和在加密和解密器件中同步. 因为数据是逐位加密的,所以初始化和保持同步就没有按块级加密的缺点.

在一个推荐的实施例中,供给第二个伪随机序列的装置供应独立于创立在节点和网络单元之间的虚拟电路的第二个序列,并以相当于有关虚拟电路上传送信元的速率提供这个序列.

供给第二个伪随机序列的装置,供应独立于建立在节点和网络单元之间的虚拟电路的第二个序列,并以相当于有关虚拟电路上传送信元的速率提供这个序列.

上述器件产生一个独立于各虚拟电路的同步伪随机序列,每个单元有至少创立一个通向节点的虚拟电路. 这样可以使每个虚拟电路独自地同步.

因而虚拟电路之间的时差不会带来任何问题.

在一个推荐的实施例中,供给第二个伪随机序列的装置包含一个由执行线性功能的逻辑电路环组成的移位寄存器,和供应含有至少放在该寄存器的一级中的数值的样本.

供给第二个伪随机序列的装置,包含一个由执行线性功能的逻辑电路环组成的移位寄存器,和由加 密器件供应并装载到该寄存器的至少一级中用来同步的样本.

上述器件的优点是用很简单的电路就能实现加密和解密的同步.

在一个推荐的实施例中,加密器件还包含有如下的装置:

- 记存许多密钥,
- 决定改变密钥,和
- 向各信元插入指出信元传送的密钥那些是用来对信息单元加密的信息,和

解密器件还包含有:

- 记存许多密钥的存储装置;
- 接收各加密信元传送的信息并指出那些密钥是用来对由该信元传送的信息单元加密的装置;和
- 按照在信元中传送的信息指示读取在储存器中的密钥并送往提供第一个伪随机序列的装置中.

通过下面的叙述和配图,将更清楚了解本发明和它其他特性.

图 1 表示含有上述一个无源光学网络的一个电信网络分支点方框图.

图 2 表示本发明一个加密器件和一个解密器件的一个实施例方框图.

图 3 表示一个加密器件的本实施例的部份方框图.

图 4 表示一个解密器件的本实施例的部份方框图.

图 5 和 6 表示在本发明中用来在加密器件和解密器件中实现非线性加密算法的逻辑电路的一个实施例的方框图.

图 2 表示本发明一个加密器件 CD 的一个实施例和一个解密器件 DD 的一个实施例方框图. 器件 CD 装在耦合器件 TUAN 中,器件 DD 重复地装在每个网络单元 ONU1 、.... ONU4 中. 图 2 只表示出这两个器件间由无源光学网络 APON 支持的逻辑连接而不是物理连接.

这些连接是:

- 从节点向所有单元传送已加密信息单元的连接 CT;
- 从节点向所有单元传送同步伪随机序列样本的同步连接 SYN;
- 在两个方向传送传递密钥和认可这个传递的消息的双向连接 KT;和
- 为了把现用的密钥换成已存在解密器件的储存器中的密钥指定从节点 OAN 到单元 ONU1 路径传送的高速连接 KS.

这些独立的连接实际上都由同一个信元支持. 建立起独立的虚拟电路从节连接到各个单元. 在从节连接到各个单元的方向,每个信元包含有五个八位位组的信头和 48 个八位位组的有效负载,它的第一个八位位组用作序列号 SN,随在指定的虚拟电路上每发送一个信元而增加,第二个八位位组,或者控制八位位组,用作指明加密和解密操作的服务信息. 其余 46 个八位位组传送信息单元,每个信息单元占有全部八位位组.

加密器件用各自的密钥对派送往网络单元 ONU1 、.... ONU4 的信息单元加密. 它包含:

- 一个输入终端 1 接收要加密的二进制数据流,定是由要发送的信元的信息单元的数位经成的,短个信息单元是一个电话线路样本的数值,或者是要送到任何一个单元 ONU1 、.... ONU4 的一个数据微包;信元传送的信头位和服务位不要加密;
- 一个输入终端 7 接收虚拟电路识别符 VCI 和虚拟路径识别符 VPI,这两个识别符识别由被发送信元支持的虚拟电路,和把节点 OAN 连接到单元 ONU1;
- 一个输入终端 8 接收支持该虚拟电路的信元序列中该信元的序列号 SN;
- 一个输入终端 9 接收一个二进制字 BP,它指示其中一位正在发送和解密的八位位组在该信元中的位置.
- 一个输出终端 3 向逻辑连接 CT 供应已加密的位流;
- 一个输出终端 4 向同步逻辑连接 SYN 供应同步伪随机二进制序列的样本;
- 一个输入-输出终端 6 接收和传送逻辑连接 KT 上的传递和认可密钥的消息;

- 一个输出终端 17 接向输送命令使用新密钥的消息的高速连接 KT;

- 一个异或门 EXOR1,有第一个输入接到输入终端 1,第二个输入接收一个非线性伪随机二进制序列 NLS1,和一个输出接到输出终端 3,这个门以 on the fly 方式,即以逐位方式对信息单元加密.

- 一个逻辑电路 NFL1 执行非线性的逻辑功能因而难以逆运算,这个电路 NFL1 有第一个输入接收一个线性伪随机二进制序列 LS1,第二个输入接收一个密钥 Ki,第三个输入接收二进制字 BP,第四个输入接收一个位 KNL,它起码是一个密钥数的标出密钥 Ki 的一个有意义位,和向 EXOR1 逐位供应非线性伪随机序列的输出;

- 一个密钥储存器 KM,可以为各单元 ONU1 、.... ONU4 储存两个密钥数(一个正在用的密钥和一个相反的密钥),并有连到逻辑电路 NFL1 的第二个输入的输出;

- 一个控制器 CDC 控制整个加密器件的工作,并实施密钥改变的约定,这个控制器有一个输入-输出端连接输入-输出终端 6,一个连接密钥储存器 KM 输入的输出端,用来向该储存器写入新的密钥,并命令读出为各信息单元加密用的密钥,一个连接逻辑电路 NLF1 第四个输入,向它供应 KNL 位的输出端,和一个连到输出终端 17 的输出端;和

- 一个同步器件 SD1,它含有许多伪随机二进制序列发生器,分别用在各自的虚拟电路,含有一个为虚拟电路提供和被加到输入终端 7 的识别符 VPI-VCI 识别的序列 LS1i 的发生器 SD1i,这个器件 SD1 有一个接到输入终端 7 的输入端用来接收标识符对 VPI-VCI,一个接到输入终端 8 的输入端用来接收序列号 SN,一个第一输出端向逻辑电路 NFL1 的第一输入端供应线性伪随机二进制序列 LS1,和一个接到输出终端 4 的第二输出端,和为网络单元中的解密器件同步周期地提供线性伪随机二进制序列 LS1 的样本,现用的数据必须通过它来加密和发送.

EXOR 门逐位处理要加密的数据,因而没有任何时延. 每个信息单元含有全部八位位组的数. 因此至少对一个八位位组来说,密钥 Ki 维持不变. 逻辑电路 NLF1 因此逐个八位位组工作,控制器 CDC 对每个八位位组合理地改变密钥 Ki . 逻辑电路 NLF1 一次地计算序列 NLS1 的一个八位位组,但逐位地以加密的比特率输出到 EXOR1 门的第二个输入端.

如果打算用无源光学网络APON只传送通常的信元,每个信元的内容也只通过一个网络单元,电路 NLF1 自然能够应付信元的速率,也就是说,能为46个八位位组的块计算出线性伪随机序列 NLS1,因为标准的信元有效负载的长度是48个八位位组,另两个八位位组用作服务信息.

同步器件 SD1 有和在节点 TUAN 和网络单元 ONU1 、.... QNU4 之间建立的虚拟电路数目相同的开动的发生器. 每个发生器以信元速率提供一个伪随机序列支持和该发生器相应的虚拟电路. 每当序列数 SN 因虚拟电路的一个单元增加时就由 VPI-VCI 识别,为该虚拟电路提供的序列为前移一位. 它是由序列的25个连续的位组成一个字的形式并行地供应的.

每个发生器,例如 SD1i,以信元速率向同步连接 SYN 供应各含一位数的两个样本,支持和该发生器相应的虚拟电路.

序列 NLS1 是一个非线性序列,因为它是由一个执行非线性逻辑函数的逻辑电路 NLF1 产生的. 由于这样非线性,即使知道这个非线性函数也很难从序列 NLS1 的部份确定密钥 Ki .

序列 LS1i 等是线性的,因为它们是由执行全部线性函数的逻辑电路产生的. 这些函数使用例如由异或门建立的线性算子. 这一类线性函数对企图欺诈地解密是没有多大抵抗的,但是比较容易同步两个必须同时产生同样序列的器件,一个在加密器件中和另一个在解密器件中.

本发明的解密器件 DD 的实施例包含:

- 一个连到逻辑连接 CT 接收已加密位流的输入端 10;

- 一个连接到同步逻辑连接 SYN 接收线性伪随机序列 NLS1 的输入端 11;

- 一个连到逻辑连接 KT 和加密器件 CD 交换密钥传递消息的输入-输出端 12;

- 一个连到连接 KS 接收密钥命令的输入端 18;

- 一个接收端 14,接收虚拟电路识别符 VCI 和虚拟路径识别符 VPI,识别现在发送和解密的信元支持的虚拟电路;

-一个接收该虚拟电路中该信元的序列号 SN 的输入端 15;

- 一个接收端 16,接收二进制字 BP,它指示其中一位正在发送和解密的八位位组在该信元中的位置;

- 一个提供解密位流的输出端 13;

- 一个异或门 EXOR2,它的第一个输入接到输入终端 10 接收加密数位流,第二个输入接收一个非线性伪随机二进制序列 NLS2,当需要同步时,它和 NLS1 相同而且同步,和一个接到输出终端 13 的输出 端,这个门以逐个位方式对已加密的位解密;

- 一个和逻辑电路 NLF1 相同并执行同样的非线性逻辑函数的逻辑电路 NLF2,它的第一个输入当需要同步时,接收和序列 LS1i 相同的线性伪随机序列 LS2i,第二个输入接收含有有关解密器件 DD 的网络单元特有的密钥 Ki,第三个输入接到输入终端 16,接收指示其中一位正在解密的八位位组在该信元中的位置的二进制字 BP,第四个输入接收 KNL 位,它至少是一个密钥数中有意义的位,标明密钥 Ki 正在使用,NFL2 的输出端逐位地向 EXOR2 门的第二个输入供应非线性伪随机序列 NLS2;

- 一套各自含一个密钥的双寄存器 KR,其中一个是有关解密器件正在用的密钥 Ki,这套寄存器在连接电路 NLF2 的第二个输入的输出端,供应储存在 KR 中两个密钥之一个;

- 一个同步器件 SD2,它含有许多伪随机二进制序列发生器,分别用在各个建立在节点 TUAN 和包含该解密器件 DD 的网络单元之间的的虚拟电路,特别是一个解密器件 SD2i 为 VPI-VCI 识别的虚拟电路供应序列 LS2i. 该装置ＳＤ２有一个输入连到输入端１１可以接收ＶＰＩ－ＶＣＩ这对识别符，一个输入连到端子１５以接收当前被解密的信元的序列号ＳＮ，还有一个输出向逻辑电路ＮＬＦ２的第一输入供给线性伪随机二进制序列ＬＳ２ｉ；以及

－一个控制器ＤＤＣ，有一个输入－输出连接到输入－输出端子１２以和控制器ＣＤＣ交换密钥改变记录信息，一个输出连接到密钥寄存器ＫＲ的控制输入以在决定更新有关网络单元的密钥时向该寄存器提供一个新的密钥值，还有一个向电路ＮＬＦ２的第四输入供给ＫＮＬ位的输出.

在各个不同的网络单元ＯＮＵ１、…、ＯＮＵ４的每个解密器件中,每个时候的密钥Ｋｉ都是不同的．即或一个单元专有的密钥已经泄漏了，为了保密每个虚拟电路的加密密钥还是周期性地改变，例如每１５分钟一次.

每１５分钟控制器ＣＤＣ向网络单元ＯＮＵ１、…、ＯＮＵ４的所有解密器件ＤＤ送出一个信息，要求它们每个提供一个新的密钥．该消息包含指示要建立的一套新密钥的一个号码．同时，控制器ＣＤＣ开动一个重复定时器，时间长达回答所有网络单元所需最长时间．如果哪个单元在这时间内未作回答，控制器便向那个单元重发消息．

如果连续试三次都不成功，控制器ＣＤＣ便认为该单元损坏而向它发出不认可消息．

在正常情况下，当每个解密器件的控制器ＤＤＣ收到这一消息，便随机抽出一个新密钥送给控制器ＣＤＣ，同时指出新的一组密钥的号码并用一个误差检测码保护密钥．这可以用明文发出，因为无源光学网络ＡＰＯＮ的定向性能可以保证在网络单元至节点方向传递的保密．每个密钥伴随有一个循环冗余误差检测码字．

如果密钥被无误接收，控制器ＣＤＣ便发出认可消息并将新密钥写入密钥存储器ＫＭ中相应于送出密钥的网络单元也相应于该组密钥的号码的处所．此时它还是一个预备密钥．

控制器ＤＤＣ并不立即将新密钥写入一个寄存器ＫＲ，因为它必需首先确信密钥已被加密器件ＣＤ接收到．当控制器ＤＤＣ送出一个新密钥，它便要开动一个时间比重复定时器的更长的定时器．如果没有收到任何不认可或任何邀请提供密钥的新消息，它便认为当定时器走完时它送出的密钥便已收到．那时它便将密钥存储到ＫＲ组中两个寄存器的相应于新的一组密钥号码的一个中．这期间正在用于解密的密钥Ｋｉ是存储在ＫＲ组的另一个寄存器中．

在每个加密信元中，包含着加密和解密特有的服务信息的控制八位位组,其中有两位用于以一个号码来指定加密器件正在使用的密钥组、两位分别用于两个同步取样、四位用于一个误差检测码字．此误差检测对于避免传递误差最终引起解密器件中密钥的变动是很重要的．

决定使用存在存储器ＫＭ和集合ＫＲ中的新的一组密钥的是加密器件中的控制器ＣＤＣ．包括用来将一个信元译码的密钥的组号以明文在此信元中传递．此密钥号为当前正用于加密的密钥组中的全部密钥所共有．换言之，为所有网络单元ＯＮＵ１、…、ＯＮＵ４所共有．对于所有建立了

的虚拟电路,加密密钥实际上是同时改变的．但所有虚拟电路解密用的密钥则不是绝对同时改变的，因为在每个网络单元控制器ＤＤＣ并不改变解密密钥，直至它接收到包含有一个新密钥号的信元为止．

使用定期向解密器件ＤＤ传递同步取样的控制八位位组有很大好处．这样不仅能快速取得同步，而且能快速检测同步的变坏，也能更新密钥．

为节点ＯＡＮ和任何网络单元之间建立的每个虚拟电路都提供有单独的发生器ＳＤ１ｉ和ＳＤ２ｉ．此装置的好处是每次不同步只影响一个虚拟电路．例如，每个耦合装置ＴＵＡＮ包括一个加密器件ＣＤ，后者则含有４４个ＳＤ１ｉ这样的发生器，而每个网络单元ＯＮＵ１、…、ＯＮＵ４包括１０个ＳＤ２ｉ这样的发生器，使得每个网络单元能用耦合装置ＴＵＡＮ建立十个左右的虚拟电路．

给出识别符ＶＣＩ和ＶＰＩ、序列号ＳＮ、在耦合装置ＴＵＡＮ和每个网络单元ＯＮＵ１、…、ＯＮＵ４中的位置ＢＰ的装置是通常的信号传输装置，其实现每个该种技术的熟练人员都是很清楚的．

图３表示出发生器ＳＤ１ｉ的一个实施例的方块图．该发生器是同步装置ＳＤ１的一部分并相应于标有ＶＰＩ－ＶＣＩ的一个虚拟电路．

此实施例包括:

－一个包括２５级Ｑ１、…、Ｑ２５的移位寄存器，每级有一个数据输入、一个直接连到下一级的数据输入的输出、和一个接收时钟信号的控制输入（图中未画）；

－一个输出，并行供给一个２５位的字，这２５位是线性序列ＬＳ１ｉ的连续位，取自相应的２５级Ｑ１、…、Ｑ２５的输出;

－一个异或门ＥＸＯＲ３，其一个输入连到Ｑ２５级的输出，一个输入连到Ｑ３级的输出，而一个输出连到寄存器的第一级Ｑ１的数据输入;以此方式连接，该门构成一个发生器多项式$1+X^{3}+X^{25}$的一个线性反馈回路；以及

－一个控制寄存器Ｑ１、…、Ｑ２５和送出同步取样的装置ＳＳ，包括一个连接到门ＥＸＯＲ３的输出以对序列ＬＳ１ｉ的一个值Ｓ１进行取样的第一输入、一个连接到第１２级Ｑ１２的输出以对序列ＬＳ１ｉ的一个值Ｓ２进行取样的第二输入、一个连接到输入端子８以接收序列号ＳＮ

的第三输入、一个输出（未画），当每次序列号ＳＮ增加１个单位时同时向所有的级Ｑ１、…、Ｑ２５提供一个时钟信号、和一个输出，向连接到同步逻辑连接ＳＹＮ的输出端子４提供样本对Ｓ１、Ｓ２的输出.

当作好一个新的连接，即当建立了一对新的识别符ＶＰＩ－ＶＣＩ，一个新的同步装置ＳＤ１ｉ便从一个有线装置规定的固定值进行初始化.实际上同时一个同步装置ＳＤ２ｉ被随机初始化.接着装置ＳＤ２ｉ从逻辑连接ＳＹＮ传送的取样开始被同步.支持新连接的每个信元在其有用负数中包括两个样本Ｓ１和Ｓ２，在控制８位位组中包括加密和解密操作特有的服务信息.

因为每个包含有一位的两个取样是这样在支持有关的虚拟电路的每个信元中传送的，因此必需等待正好传递１３个信元才可能在解密器件ＤＤ中重建一个２５位的、和同时由同步装置ＳＤ１ｉ产生的序列相同的序列，并在以后能够通过以信元来到的速率将它激活而使它自动工作.

图４表示作为同步装置ＳＤ２一部分的发生器ＳＤ２ｉ的一个实施例的方块图.这个实施例包括:

－一个包括２５级Ｑ１'、…、Ｑ２５'的移位寄存器，每级有一个数据输入、一个控制输入（未画）、和一个输出;

－一个异或门ＥＸＯＲ３'，它有一个输入端连接到Ｑ２５'级的输出端、一个输入端连接到Ｑ３'级的输出端、和一个输出端;

－一个逻辑电路ＳＷ１，它等效于一个开关，有两个输入端ａ和ｂ和一个输出端.输入端ａ被连到门ＥＸＯＲ３'的输出端而该输出端被连到第一级Ｑ１'的数据输入端;

－一个逻辑电路ＳＷ２，它等效于一个开关，有两个输入端ａ和ｂ和一个输出端.输入端ａ被连到Ｑ１２'级的输出端而该输出端被连到Ｑ１３'级的输入端;

－一个控制寄存器Ｑ１',…,Ｑ２５'和同步的电路ＳＳ'.它有一个输入被连接到输入端１１以接收经逻辑连接ＳＹＮ传递的同步样本Ｓ１和Ｓ２、一个输入连接到输入端１４以接收每个信元的序列数ＳＮ、一个输入连到移位寄存器第１２级Ｑ１２'的输出端以对序列ＬＳ２ｉ的样品Ｃ２进行取样、一个输入端被连到门ＥＸＯＲ３'的输出端以对序列ＬＳ２ｉ的

样品C1进行取样、一个同时向寄存器所有各级Q1'、…、Q25'提供一个时钟信号，每次使序列数SN增加1个单位的输出端（未画）、一个输出端连接到电路SW1的输入端b以提供加密器件CD送来的样品S1、一个输出端连接到电路SW2的输入端b以提供加密器件CD送来的样品S2、和两个输出端分别连接到电路SW1和SW2的控制输入端.

在同步相位中电路SS'控制开关电路SW1和SW2使得每个电路的输出端都和输入端b连到.这样,样品S1供给第一级Q1'而样品S2供给第13级Q13'.在有关虚的拟电路收到13个连续的有效信元后，26个样品被相继存储进了移位寄存器Q1'、…、Q25'.它包含的这个25位的序列便等同于加密器件CD中的同步装置SD1i的移位寄存器Q1、…、Q25中包含的序列.这样便获得了同步.

这时电路SS'使得每个开关装置SW1和SW2将其输入端a和输出端连到.而移位寄存器Q1',…,Q25'和门EXOR3'则与同移位寄存器Q1、…、Q25和门EXOR3的情况完全一样地构成回路.这两个移位寄存器按信元传递的速率对好时钟，因而,如果在线路上没有可能在序列数SN的传递中产生误差的干扰的话便能继续产生同样的序列LS1i和LS2i.

收到的样本S1和S2由电路SS'和在移位寄存器Q1'、…、Q25'处取样的值C1和C2系统地进行比较.如果电路SS'探测到若干误差大于一个固定阈值便得出结论同步过程必需重新开始，并令每个开关电路SW1和SW2将其输入端b和其输出端相连.

对于每个信元,电路SS'将该信元的序列数SN和一个预期序列数SNe及一个预期序列数加1进行比较以探测信元的任何损失:

-如果SN=SNe，接收到的信元用移位寄存器Q1'、…、Q25'的当前态进行解密.电路SS'通过检查包含在控制八位位组中的误差探测字的4位而检查包含着加密和解密信息的控制八位位组的有效性:

--如果控制八位位组被接受,电路SS'将取样S1和S2的值和取样C1和C2的值相比并用一误差计数器对任何不符进行计数.

---如果在接收的最后13个控制八位位组中探测到S1、S2和C1、C2之间的不符不多于一个，电路便输出一个时钟信号命令在移位

寄存器Q1'、…、Q25'中移动一步．之后电路等待接收下一个信元．该信元将使用这移动产生的序列LS2i的新值进行解密．

－－－如果在接收的最后13个控制八位位组中探测到S1、S2和C1、C2之间的不符达两个或两个以上个，电路便重新开始同步过程．也就是它让每个开关电路SW1和SW2将其输入端b连到其输出端．这样，取样S1和S2的值可以输入Q1'和Q13'两级使移位寄存器在一段相应于接收携带13对新取样的13个信元的时间延迟后全部重新初始化．

－－如果控制八位位组由于检查其4个误差探测位给出否定结果而被否决，这时误差计数器仍然不变，因为样本S1和S2不能使用．电路SS'供给一个时钟信号便能一步改变移位寄存器Q1'、…、Q25'的内容，然后等待接收下一个信元．

－如果SN＝SNe＋1，这便意味着信元数SN＝SNe已丢失．电路SS'命令在移位寄存器Q1'、…、Q25'中移动一步，之后信元使用移位寄存器的新状态进行解密，其后控制八位位组象在SN＝SNe的情况下一样处理．

－如果SN≠SNe且SN≠SNe＋1，电路SS'通过输入一个包含在接收到的信元中的数值提供一个预期序列数SNe使计数器重新初始化；之后即重新开始同步过程．

图5表示一个逻辑电路NLF1的一个实施例的方块示意图．该实施例包括：

－6个子集SA0、SA1、SA2、SA3、SA4、SA5分别相应于要使用的非线性函数的6个相继的计算步骤．其中三个偶数子集SA0、SA2、SA4彼此相同而三个奇数子集SA1、SA3、SA5彼此相同；

－一个压缩装置CD有两个输入端，每个接收一个32位字，有一个输出端供给一个只有8位的、运用常规的循环冗余码字的计算方法、例如通过以多项式$X^8 + X^2 + X + 1$作除法运算取其余数获得的字；

－一个8位移位寄存器SR，有一个输入端连接到压缩装置CD的输出端以获得并行的8位；有一个输出端串行输出8位，构成非线性伪随机

序列ＮＬＳ１；以及

一个控制单元ＣＵ输出时钟信号经未画出的联线给所有子集ＳＡ０、…、ＳＡ５和移位寄存器ＳＲ．

对j=0至5,每个子集SAj包括:

－一个输入端，接收一个３２位二进制字．后者由三个二进制字并行连接组成：ＫＮＬ位，这是键数的最不重要的位；６位的二进制字ＢＰ，表示要加密的８位位组在包含此８位位组的信元中的位置；和一个由线性伪随机序列发生器电路ＳＤ１ｉ提供的线性伪随机序列ＬＳ１ｉ的２５个连续位组成的２５位二进制字;

－一个第二输入端，接收一个包含键Ｋｉ的３２位二进制字;

－一个第三输入端，接收一个３２位二进制字．后者由第（ｊ－１）个子集（其中ｊ≥１）的第一输出端提供、由二进制字ＫＮＬ、ＢＰ、ＬＳ１ｉ为子集ＳＡ０而组成的;

－一个第四输入端，接收一个３２位二进制字．后者由第（ｊ－１）个子集（其中ｊ≥１）的第二输出端提供、由键Ｋｉ为子集ＳＡ０而组成；以及

－两个输出端，每个提供３２位、且连到第（ｊ＋１）个子集（其中ｊ＝０至４）的第三和第四输入端．子集ＳＡ５的两个输出端连到压缩装置ＣＤ的两个输入端．

控制单元ＣＵ命令以８位并行和以要加密的８位位组的定时率输入寄存器ＳＲ，同时命令以要加密的位的定时率进行读出．

图６表示两个相邻子集ＳＡｊ和ＳＡｊ＋１（其ｊ取偶数值）的方块示意图．子集ＳＡｊ包括:

－一个向右旋转装置３３，移位为δｊ且一个输入端连接到子集ＳＡｊ的第四输入端而输出端输出３２位;

－一个３２个或非门３４的集合，每个门有一个输入连接到装置３３的输出端的一位，一个输入连接到子集ＳＡｊ的第三输入端，而一个输出构成集合３４的一个输出位;

－一个向右旋转装置３５对于移位δ_{j+1}，有一个输入端连到子集ＳＡｊ的第一输入端以接收由二进制字ＫＮＬ、ＢＰ、ＬＳ１ｉ连到而成的３

2位，还有一个32位输出；

－一个32个异或门36的集合，每个门有一个输入连接到集合34的一个门的输出，一个输入连接到右旋装置35的输出端处的一位，还有一个输出构成子集SAj的第一输出的一位；

－一个左旋转装置37对于移位为δj，有一个输入连接到子集SAj的第三个输入以接收由二进制字KNL、BP、LS1i连到而成的32位，还有一个32位输出；

－32个与非门的一个集合38，每个门有一个输入连接到左旋转装置37的输出处的一位，一个输入连接到子集SAj的第四输入处的一位，还有一个输出构成集合38的一个输出位；

－一个移位δ_{j+1}的向右旋转装置39，有一个输入构成子½SAJ的第二个输入且接收密钥Ki的32位，还有一个32位输出；

－32个异或门的一个集合40，每个门有一个输入连接到右旋转装置39的输出处的一位，一个输入连接到集合38的一个门的输出，还有一个输出构成子集SAj的第二个输出的一位.

子集SAj+1包括

－一个移位为 δ_{j+1}的左旋转装置41，有一个输入连接到x*集SAj+1的第三个输入以接收一个32位二进制字£*还有一个32位输出；

－32个或非门的一个集合42，每个门有一个输入连接到子集SAj+1的第三个输入的一位，一个输入连接到左旋转装置41的输出处的一位，还有一个输出构成集合42的一个输出位；

－一个移位 $\delta_{j+1}+1$的向右旋转装置43，有一个输入联连到子集SAj+1的第二个输入以接收密钥Ki的32位二进制字，并有一个32位输出；

－32个异或门的一个集合44，每个门有一个输入连接到集合42的输出处的一位，一个输入连接到右旋转装置43的输出处的一位，还有一个输出构成子集SAj+1的第一个输出处的一位；

－一个移位为 δ_{j+1}的左旋转装置45，有一个输入连接到集SAj+1的第四个输入以接收一个32位字，还有一个32位输出；

－32个与非门的一个集合46，每个门有一个输入连接到子集SAj

+ 1 的第四个输入处的一位，一个输入连接到左旋转装置 4 5 的输出处的一位，还有一个输出构成集合 4 6 的一个输出位；

- 一个移位 $\delta_{j+1}+1$ 的向右旋转装置 4 7，有一个输入连到子集 S A j + 1 的第三个输入处以接收由二进制字 K N L、B P、和 S 1 i 连到而成的 3 2 位二进制字，还有一个 3 2 位输出；以及

- 3 2 个异或门的一个集合 4 8，每个门有一个输入连接到集合 4 6 的一个输出位，一个输入连接到右旋转装置 4 7 的一个输出位，还有一个输出构成子集 S A j + 1 的第二个输出的一位。

在此实施例中：

- δ_0 值等于零.

- 对于 $j \geq 1$， δj 值等于 2^{j-1}

向右位移装置 3 5、3 9、4 3、4 7，向左位移装置 3 3、3 7、4 1、4 5，和压缩装置 C D 进行实际上不可逆的运算. 因此一个“盗版者”就是清楚知道一部分，甚至很大一部分，也很难找到密钥. 每个门、每个向右或向左位移的逻辑电路、和压缩装置 C D 的实现都是完全按常规的.

说 明 书 附 图

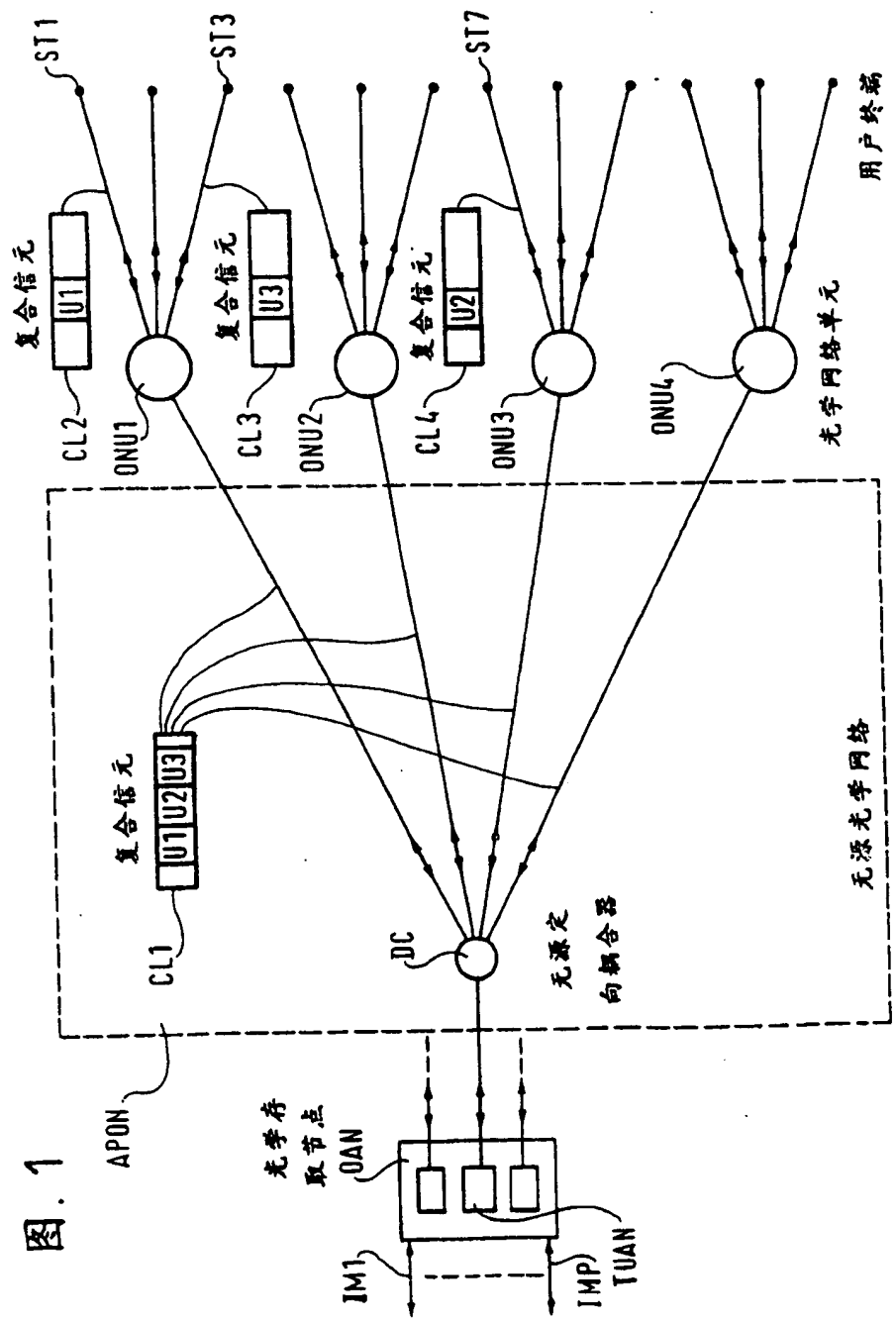

ST1
ST3
ST7
用户终端
复合信元
U1
U3
U2
CL2
CL3
CL4
ONU1
ONU2
ONU3
ONU4
光学网络单元
复合信元
U1 U2 U3
CL1
DC
无源光学网络
无源定向耦合器
APON
光学存取节点
OAN
IM1
IMP
TUAN

图. 1

图 2

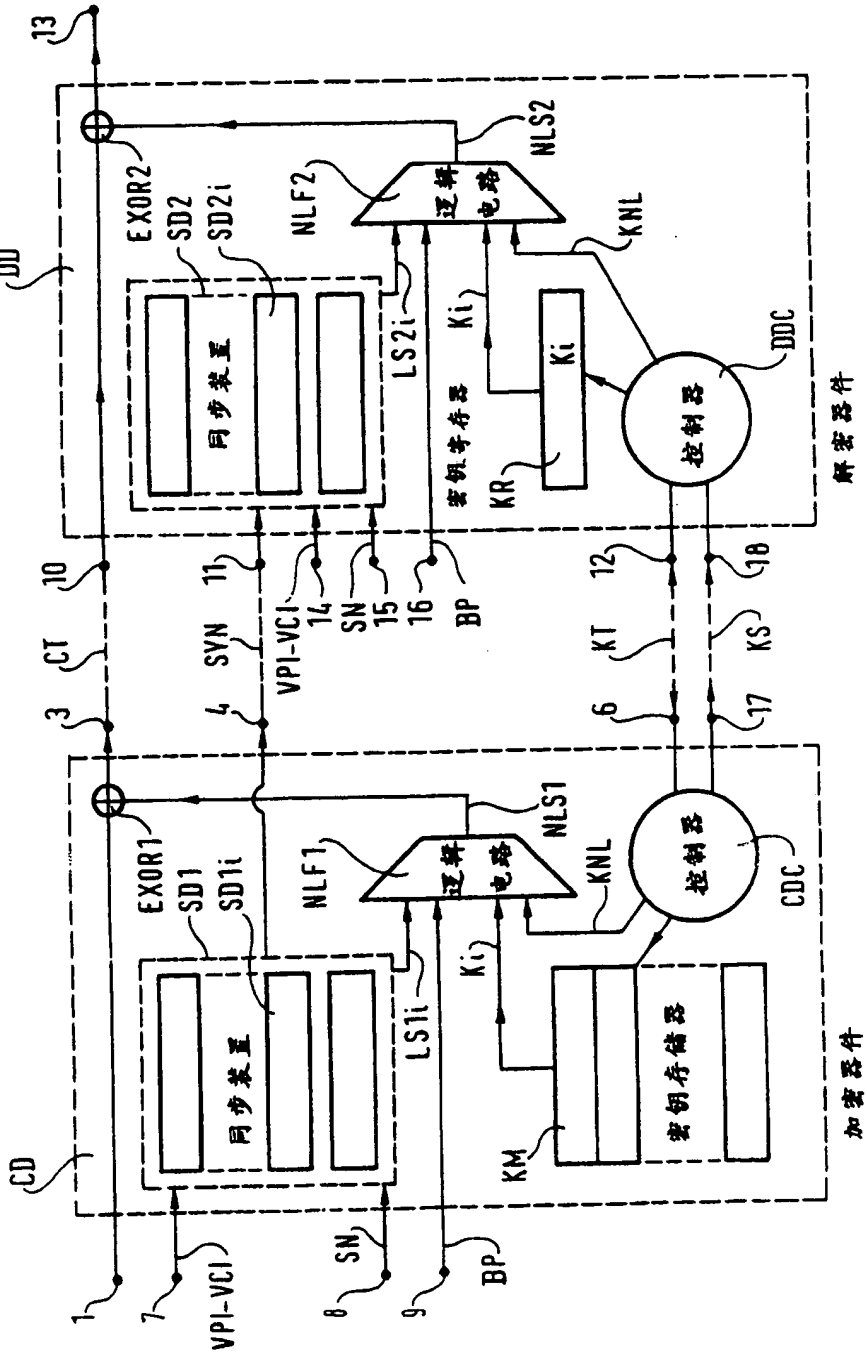

CD
DD
CDC
DDC
KM
KR
KNL
Ki
Ki)
LS1i
LS2i
NLF1
NLF2
NLS1
NLS2
EXOR1
EXOR2
SD1
SD1i
SD2
SD2i
同步装置
逻辑电路
控制器
密钥存储器
加密器件
解密器件
VPI-VCI
SN
BP
SYN
CT
KT
KS
1
3
4
6
7
8
9
10
11
12
13
14
15
16
17
18

图 3

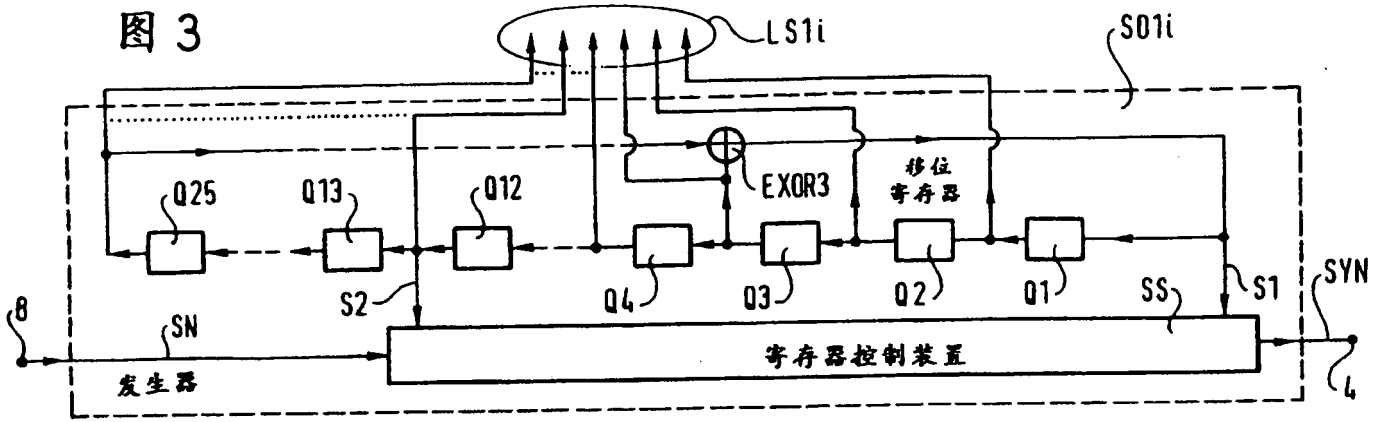

LS1i
SO1i
EXOR3
移位
寄存器
Q25
Q13
Q12
Q4
Q3
Q2
Q1
S2
SS
S1
SYN
8
SN
寄存器控制装置
发生器
4

图 4

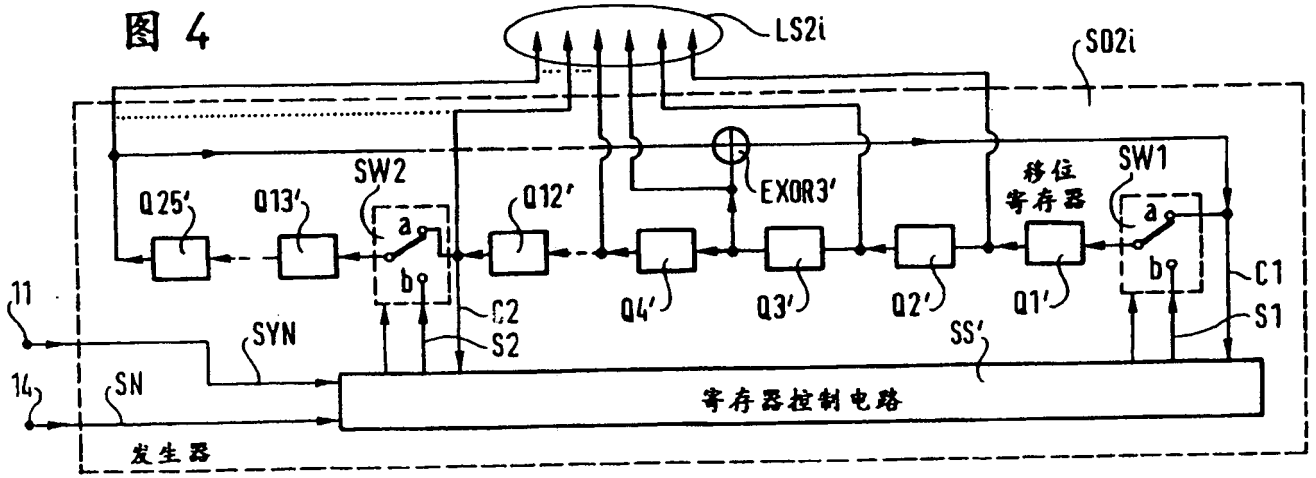
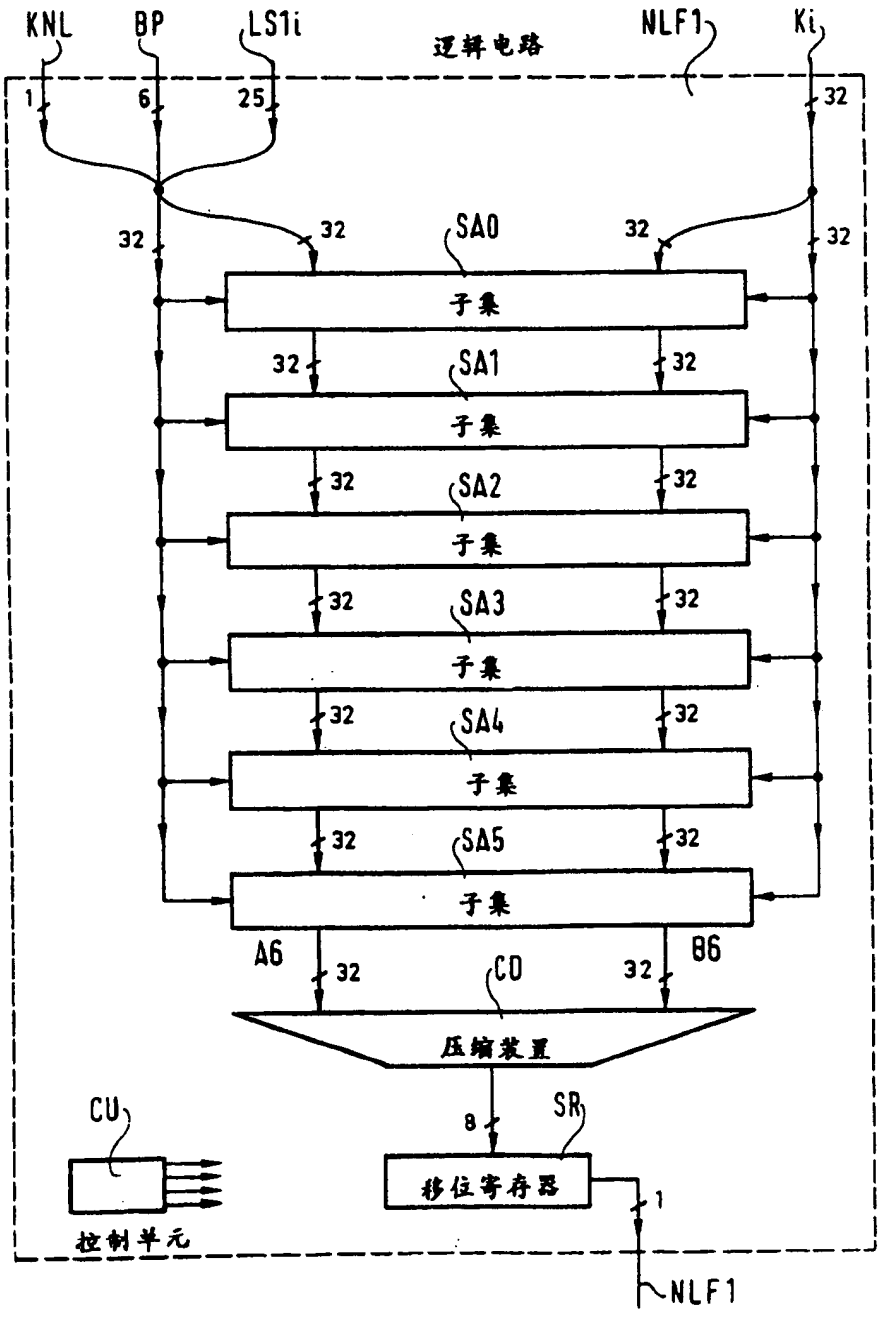

LS2i
SO2i
SW2
SW1
EXOR3'
移位
寄存器
Q25'
Q13'
Q12'
Q4'
Q3'
Q2'
Q1'
a
b
C2
S2
C1
S1
SS'
11
SYN
14
SN
寄存器控制电路
发生器

图 . 5


KNL
BP
LS1i
逻辑电路
NLF1
Ki
1
6
25
32
SA0
子集
SA1
SA2
SA3
SA4
SA5
A6
B6
CO
压缩装置
CU
SR
8
移位寄存器
控制单元
NLF1

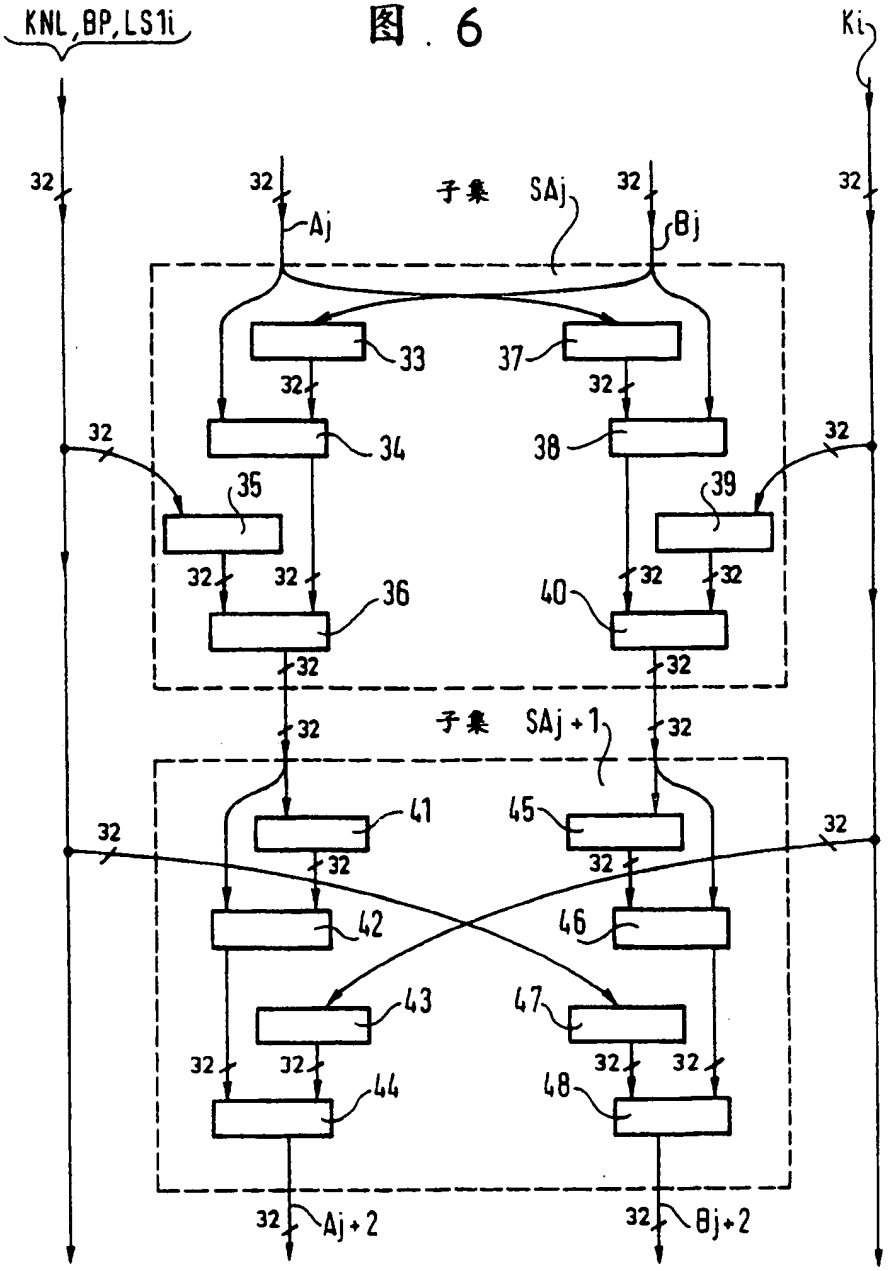

KNL, BP, LS1i
Ki
32
Aj
Bj
子集 SAj
33
37
34
38
35
39
36
40
子集 SAj+1
41
45
42
46
43
47
44
48
Aj+2
Bj+2

図 . 6